This bulletin provides a summary of new or updated vulnerabilities, exploits, trends, viruses, and trojans. **Updates to items appearing in previous bulletins are listed in bold text.** The text in the Risk column appears in red for vulnerabilities ranking High. The risks levels applied to vulnerabilities in the Cyber Security Bulletin are based on how the "system" may be impacted. The Recent Exploit/Technique table contains a "Workaround or Patch Available" column that indicates whether a workaround or patch has been published for the vulnerability which the script exploits.

Bugs, Holes, & Patches

- Windows Operating Systems
  - 21-6 Productions Orbz Password Field Buffer Overflow
  - Alt-N MDaemon Privilege Escalation
  - CoffeeCup Direct/Free FTP ActiveX Component Remote Buffer Overflow
  - DeSofto MyProxy Arbitrary Ports & Hosts Connection
  - InnerMedia DynaZip Library Buffer Overflow
  - IpSwitch WS_FTP Buffer Overflow
  - LucasArts Star Wars Battlefront Game Server Remote Denials of Service
  - MailEnable Stack Overflow & Pointer Overwrite
  - Microsoft Internet Explorer Infinite Array Sort Denial of Service
  - Microsoft Internet Explorer 'Save Picture As' Image Download Spoofing
  - Microsoft WINS Memory Overwrite
  - **Microsoft Windows Shell Remote Code Execution (Updated)**
  - Mozilla Firefox Infinite Array Sort Denial of Service
  - **Nullsoft Winamp 'IN_CDDA.dll' Buffer Overflow (Updated)**
  - Pegasus Mail Mercury Mail Transport System Buffer Overflow
  - **Symantec LiveUpdate Zip Decompression Routine Denial of Service (Updated)**
  - VMWare Workstation Format String
  - WeOnlyDo! wodFtpDLX ActiveX Component Remote Buffer Overflow
  - Win FTP Server Information Disclosure
  - YoungZSoft CMailServer Multiple Vulnerabilities
- UNIX / Linux Operating Systems
  - ACPID Insecure Umask Directory Permissions
  - **Apache mod_ssl SSLCipherSuite Access Validation (Updated)**
  - **Apache mod_include Buffer Overflow (Updated)**
  - Apple iCal Calendar Import Alarm Notification Failure
  - Apple Safari Web Browser Infinite Array Sort Denial of Service
  - Atari800 Emulator Multiple Buffer Overflows
  - EnergyMech ESAY Command Buffer Overflow
  - **GD Graphics Library Remote Integer Overflow (Updated)**
  - **GNU a2ps Command Injection (Updated)**
  - **GNU InetUtils TFTP Client Remote Buffer Overflow (Updated)**
  - **ImageMagick Remote EXIF Parsing Buffer Overflow (Updated)**
  - **Info-ZIP Zip Remote Recursive Directory Compression Buffer Overflow (Updated)**
  - IPCop 'proxylog.dat' Cross-Site Scripting
  - Jabber Server Multiple Remote Buffer Overflows
  - Mozilla Camino Web Browser Infinite Array Sort Denial of Service
  - **Mozilla Bugzilla Multiple Authentication Bypass& Information Disclosure (Updated)**
  - Multiple Vendors Cyrus IMAPD Multiple Remote Vulnerabilities
  - Multiple Vendors Cyrus IMAP 'imap magic plus' Buffer Overflow
  - **Multiple Vendors Samba Remote Wild Card Denial of Service ((Updated)**

Bugs, Holes, & Patches

The table below summarizes vulnerabilities that have been identified, even if they are not being exploited. Complete details about patches or workarounds are available from the source of the information or from the URL provided in the section. CVE numbers are listed where applicable. Vulnerabilities that affect **both** Windows and Unix Operating Systems are included in the Multiple Operating Systems section.

Note: All the information included in the following tables has been discussed in newsgroups and on web sites.

The Risk levels defined below are based on how the system may be impacted:

- **High** - A high-risk vulnerability is defined as one that will allow an intruder to immediately gain privileged access (e.g., sysadmin or root) to the system or allow an intruder to execute code or alter arbitrary system files. An example of a high-risk vulnerability is one that allows an unauthorized user to send a sequence of instructions to a machine and the machine responds with a command prompt with administrator privileges.
- **Medium** - A medium-risk vulnerability is defined as one that will allow an intruder immediate access to a system with less than privileged access. Such vulnerability will allow the intruder the opportunity to continue the attempt to gain privileged access. An example of medium-risk vulnerability is a server configuration error that allows an intruder to capture the password file.
- **Low** - A low-risk vulnerability is defined as one that will provide information to an intruder that could lead to further compromise attempts or a Denial of Service (DoS) attack. It should be noted that while the DoS attack is deemed low from a threat potential, the frequency of this type of attack is very high. DoS attacks against mission-critical nodes are not included in this rating and any attack of this nature should instead be considered to be a "High" threat.

Windows Operating Systems Only

Vendor & Software Name	Vulnerability - Impact Patches - Workarounds Attacks Scripts	Common Name	Risk	Source
21-6 Productions Orbz 2.10 and prior	A vulnerability exists due to a boundary error when handling join requests. This can be exploited to cause a buffer overflow by supplying an overly long password. Successful exploitation may allow execution of arbitrary code. No workaround or patch available at time of publishing. Currently we are not aware of any exploits for this vulnerability.	21-6 Productions Orbz Password Field Buffer Overflow	High	Secunia Advisory ID, SA13327, November 30, 2004
Alt-N MDaemon 7.2	A vulnerability exists due to a failure to properly drop privileges prior to executing child process, which could let a malicious user obtain elevated privileges. No workaround or patch available at time of publishing. There is no exploit code required.	Alt-N MDaemon Privilege Escalation	Medium	SecurityFocus, November 23, 2004
CoffeeCup Software CoffeeCup Direct FTP 6.0, 6.2, CoffeeCup Free FTP 6.0, 6.2	A buffer overflow vulnerability exists due to the way long buffer file names are handled, which could let a remote malicious user execute arbitrary code. No workaround or patch available at time of publishing. An exploit script has been published.	CoffeeCup Direct/Free FTP ActiveX Component Remote Buffer Overflow	High	Secunia Advisory, SA13282, November 23, 2004
DeSofto MyProxy 6.58	A vulnerability exists because a remote malicious user can connect to the proxy and invoke the CONNECT command to connect to arbitrary ports. No workaround or patch available at time of publishing. Currently we are not aware of any exploits for this vulnerability.	DeSofto MyProxy Arbitrary Ports & Hosts Connection	Medium	SecurityTracker Alert ID, 1012322, November 24, 2004
Innermedia DynaZip prior to version 5.00.04	Releases compression library contain a buffer overflow that may allow a remote malicious user to execute arbitrary code. A bounds checking deficiency in DynaZip may allow a buffer overflow. A malicious user can exploit this vulnerability by creating a zip archive containing files with long names. The DynaZip library is used in a wide variety of applications. The vendor has released a fixed version (5.00.04): http://www.innermedia.com/dz/index.htm Currently we are not aware of any exploits for this vulnerability.	InnerMedia DynaZip library Buffer Overflow	High	US-CERT Vulnerability Note VU#582498, November 22, 2004
IpSwitch WS_FTP Server 5.03, 2004.10.14	Several vulnerabilities were reported that could permit a remote authenticated malicious user to execute arbitrary code on the target system. A remote authenticated user can trigger a buffer overflow in several FTP commands. The SITE, XMKD, MKD, and RFNR FTP commands are affected. A remote user can cause the FTP service to crash or execute arbitrary code. No workaround or patch available at time of publishing. A Proof of Concept exploit has been published.	IpSwitch WS_FTP Buffer Overflow	High	SecurityTracker Alert ID: 1012353, November 29, 2004
LucasArts Star Wars Battlefront 1.11	Multiple remote Denial of Service vulnerabilities exist due to insufficient boundary checks on 'nickname' data and the debugging functionality may be leveraged by a malicious client to trigger a server crash. No workaround or patch available at time of publishing. An exploit script has been published.	LucasArts Star Wars Battlefront Game Server Remote Denials of Service	Low	Bugtraq, November 24, 2004
MailEnable MailEnable Professional Edition v1.52, MailEnable Enterprise Edition	Two vulnerabilities exist in the IMAP service that could permit a remote malicious user to execute arbitrary code. A remote user can trigger a stack-based buffer overflow or an object pointer overwrite to execute arbitrary code on the target system. The vendor has issued a fix, available at:	MailEnable Stack Overflow & Pointer Overwrite	High	Hat-Squad Security Team Advisory, November 25, 2004

v1.01	http://mailenable.com/hotfix.asp A Proof of Concept exploit script has been published.			
Microsoft Internet Explorer 6.0, SP1&SP2	A remote Denial of Service vulnerability exists when the browser performs an infinite JavaScript array sort operation. No workaround or patch available at time of publishing. A Proof of Concept exploit has been published.	Microsoft Internet Explorer Infinite Array Sort Denial of Service	Low	Bugtraq, November 25, 2004
Microsoft Internet Explorer 6.0 with Windows XP SP2	A vulnerability exists which can be exploited by malicious people to trick users into downloading malicious files. The vulnerability is caused due to Internet Explorer using the file extension from the URL's filename when saving images with the 'Save Picture As' command and also strips the last file extension if multiple file extensions exist. This can be exploited by a malicious web site to cause a valid image with malicious, embedded script code to be saved with an arbitrary file extension. Workaround: Disable the 'Hide extension for known file types' option and add the proper extension to the file name in the File name box when saving. A Proof of Concept exploit has been published.	Microsoft Internet Explorer 'Save Picture As' Image Download Spoofing	Medium	Secunia Advisory ID, SA13317, November 26, 2004
Microsoft Windows (Me), Windows (NT), Windows (95), Windows (98), Windows (2000), Windows (2003), Windows (XP)	A vulnerability was reported that could allow a remote user to execute arbitrary code on the target system. A remote user can send a specially crafted WINS packet to the target server on TCP port 42 to modify a memory pointer and write arbitrary contents to arbitrary memory locations. No workaround or patch available at time of publishing. A Proof of Concept exploit has been published.	Microsoft WINS Memory Overwrite	High	US-CERT Vulnerability Note VU#145134, November 29, 2004
Microsoft Windows NT Server 4.0, Windows NT Server 4.0 Enterprise Edition, Windows NT Server 4.0 Terminal Server Edition, Windows 2000 Advanced Server, Windows 2000 Datacenter Server, Windows 2000 Server, Windows 2000 Professional, Windows XP Home Edition, Windows XP Professional, Windows Server 2003 Enterprise Edition, Windows Server 2003 Standard Edition, Windows Server 2003 Web Edition, Windows Server 2003 Datacenter Edition, Windows 98, Windows 98 SE, Windows ME; Avaya DefinityOne Media Servers, IP600 Media Servers, Modular Messaging (MSS) 1.1, 2.0, Avaya S3400 Message Application Server Avaya S8100 Media Servers	A Shell vulnerability and Program Group vulnerability exists in Microsoft Windows. These vulnerabilities could allow remote code execution. Updates available at: http://www.microsoft.com/technet/security/bulletin/MS04-037.mspx Bulletin updated to reduce the scope of a documented workaround to only support Windows XP, Windows XP Service Pack 1, and Windows Server 2003. Avaya: Customers are advised to follow Microsoft's guidance for applying patches. Advisories are located at the following locations: http://support.avaya.com/japple/css/japple?temp.groupID=128450&temp.selectedFamily=128451&temp.selectedProduct=154235&temp.selectedBucket=126655&temp.feedbackState=askForFeedback&temp.documentID=203487&PAGE=avaya.css.CSSLvl1Detail&executeTransaction=avaya.css.UsageUpdate() http://support.avaya.com/japple/css/japple?temp.groupID=128450&temp.selectedFamily=128451&temp.selectedProduct=154235&temp.selectedBucket=126655&temp.feedbackState=askForFeedback&temp.documentID=203487&PAGE=avaya.css.CSSLvl1Detail&executeTransaction=avaya.css.UsageUpdate() We are not aware of any exploits for these vulnerabilities.	Microsoft Windows Shell Remote Code Execution CVE Names: CAN-2004-0214 CAN-2004-0572	High	Microsoft Security Bulletin MS04-037 v1.1, October 25, 2004 US-CERT Cyber Security Alert SA04-286A, October 12, 2004 US-CERT Vulnerability Note VU#543864, October 15, 2004 SecurityFocus, October 26, 2004 **US-CERT Vulnerability Note, VU#616200, November 23, 2004**
Mozilla.org Firefox Preview Release, 0.8, 0.9 rc, 0.9-0.9.3, 0.10, 0.10.1	A remote Denial of Service vulnerability exists when the browser performs an infinite JavaScript array sort operation. No workaround or patch available at time of publishing. A Proof of Concept exploit has been published.	Mozilla Firefox Infinite Array Sort Denial of Service	Low	Bugtraq, November 25, 2004

Nullsoft Winamp 5.05	A vulnerability exists which can be exploited by malicious people to compromise a user's system. The vulnerability is caused due to a boundary error in the 'IN_CDDA.dll' file. This can be exploited in various ways to cause a stack-based buffer overflow e.g. by tricking a user into visiting a malicious web site containing a specially crafted '.m3u' playlist. Successful exploitation allows execution of arbitrary code. Update to version 5.0.6: http://www.winamp.com/player/ **An exploit script has been published.**	Nullsoft Winamp 'IN_CDDA.dll' Buffer Overflow	High	Security-Assessment Vulnerability Advisory, November 23, 2004 **SecurityFocus, November 24, 2004**
Pegasus Mail Mercury Mail Transport System 4.01	A vulnerability was reported that could allow a remote authenticated user to execute arbitrary code on the target system. The SELECT command contains a buffer overflow. A remote authenticated user can send a specially crafted command to the IMAP service to trigger the buffer overflow and execute arbitrary code. No workaround or patch available at time of publishing. A Proof of Concept exploit has been published.	Pegasus Mail Mercury Mail Transport System Buffer Overflow	High	SecurityTracker Alert ID: 1012361, November 30, 2004
Symantec Symantec LiveUpdate 1.80.19.0, 2.5.56.0	A vulnerability exists which may allow a malicious user to cause Denial of Service conditions in certain cases. Tithe LiveUpdate decompression routine does not check for uncompressed file sizes before attempting to decompress a downloaded LiveUpdate zip file and does not properly validate directory names before creating the directories on the target system. **Symantec will be adding additional capabilities to mitigate any potential actions of this nature in an update that will be available shortly**. A Proof of Concept exploit has been published.	Symantec LiveUpdate Zip Decompression Routine Denial of Service	Low	SecurityTracker Alert ID, 1012095, November 5, 2004 **Symantec Advisory, SYM04-017, November 23, 2004**
VMWare Incorporated VMWare Workstation 4.5.2	A format string vulnerability exists in the VMWare workstation executable because format specifier characters that are passed as a command line argument are not handled correctly, which could let a malicious user obtain elevated privileges. No workaround or patch available at time of publishing. Currently we are not aware of any exploits for this vulnerability.	VMWare Workstation Format String	Medium	SecurityFocus, November 23, 2004
WeOnlyDo! wodFtpDLX ActiveX component, wodFtpDLX ActiveX component 2.1.1 8	A buffer overflow vulnerability exists due to the way long buffer file names are handled, which could let a remote malicious user execute arbitrary code. Update available at: http://www.weonlydo.com/index.asp?showform=FtpDLX Exploit scripts have been published.	WeOnlyDo! wodFtpDLX ActiveX Component Remote Buffer Overflow	High	Securiteam, November 23, 2004
wftpserver.com WinFTP Server 1.x	A vulnerability exists in the 'data\user.wfd' file because user credentials are stored in clear text, which could let a malicious user obtain sensitive information. No workaround or patch available at time of publishing. There is no exploit code required.	Win FTP Server Information Disclosure	Medium	GSSIT - Global Security Solution IT Advisory, November 24, 2004
YoungZSoft CMailServer 5.2	Several vulnerabilities exist: a buffer overflow vulnerability exists in 'CMailCom.dll' in the attachment download processing, which could let a remote malicious user execute arbitrary code; a vulnerability exists due to insufficient validation of user-supplied input in certain scripts, which could let a remote malicious user execute arbitrary code; a vulnerability exists in the 'admin.asp' script due to insufficient filtering of HTML code from user-supplied input when displaying a user's personal information, which could let a remote malicious user execute arbitrary code; a vulnerability exists in 'fdelmail.asp' because a remote malicious authenticated user can inject SQL commands to delete a target user's mail metadata; and a vulnerability exists in 'addressc.asp' because a remote malicious user can inject SQL commands to delete a target user's address book contacts. No workaround or patch available at time of publishing. Currently we are not aware of any exploits for these vulnerabilities.	YoungZSoft CMailServer Multiple Vulnerabilities	Medium/ High (High if arbitrary code can be executed)	SIG^2 Vulnerability Research Advisory, November 24, 2004

[back to top]

UNIX / Linux Operating Systems Only

Vendor & Software Name	Vulnerability - Impact Patches - Workarounds Attacks Scripts	Common Name	Risk	Source
ACPID ACPID 1.0.1, 1.0.3	A vulnerability exists in ACPID due to an insecure umask, which could let a malicious user cause a Denial of Service. SuSE: ftp://ftp.suse.com/pub/suse/ There is no exploit code required.	ACPID Insecure Umask Directory Permissions	Low	SUSE Security Summary Report, SUSE-SR:2004:001, November 24, 2004
Apache Software Foundation Apache 2.0.35-2.0.52	A vulnerability exists when the 'SSLCipherSuite' directive is used in a directory or location context to require a restricted set of cipher suites, which could let a remote malicious user bypass security policies and obtain sensitive information. OpenPKG: ftp://ftp.openpkg.org/release/ Gentoo: http://security.gentoo.org/glsa/glsa-200410-21.xml Slackware: ftp://ftp.slackware.com/pub/slackware/ Conectiva: ftp://atualizacoes.conectiva.com.br/ Mandrake: http://www.mandrakesoft.com/security/advisories Fedora: http://download.fedora.redhat.com/pub/fedora/linux/core/updates/2/ RedHat: http://rhn.redhat.com/errata/RHSA-2004-562.html **SuSE: In the process of releasing packages.** There is no exploit code required.	Apache mod_ssl SSLCipherSuite Access Validation CVE Name: CAN-2004-0885	Medium	OpenPKG Security Advisory, OpenPKG-SA-2004.044, October 15, 2004 Gentoo Linux Security Advisory, GLSA 200410-21, October 22, 2004 Slackware Security Advisory, SSA:2004-299-01, October 26, 2004 Mandrakelinux Security Update Advisory, MDKSA-2004:122, November 2, 2004 Conectiva Linux Security Announcement, CLA-2004:885, November 4, 2004 Fedora Update Notification, FEDORA-2004-420, November 12, 2004 RedHat Security Advisory, RHSA-2004:562-11, November 12, 2004 **SUSE Security Summary Report, SUSE-SR:2004:001, November 24, 2004**
Apache Software Foundation Apache 1.3, 1.3.1, 1.3.3, 1.3.4, 1.3.46, 1.3.7 -dev, 1.3.9, 1.3.11, 1.3.12, 1.3.14, 1.3.17-1.3.20, 1.3.22-1.3.29, 1.3.31	A buffer overflow vulnerability exists in the 'get_tag()' function, which could let a malicious user execute arbitrary code. Gentoo: http://security.gentoo.org/glsa/glsa-200411-03.xml Slackware: ftp://ftp.slackware.com/pub/slackware/s Trustix: http://http.trustix.org/pub/trustix/updates/ TurboLinux: ftp://ftp.turbolinux.co.jp/pub/TurboLinux/TurboLinux/ia32/ **SuSE: In the process of releasing packages.** Exploit scripts have been published.	Apache mod_include Buffer Overflow CVE Name: CAN-2004-0940	High	SecurityFocus, October 20, 2004 Slackware Security Advisory, SA:2004-305-01, November 1, 2004 Gentoo Linux Security Advisory, GLSA 200411-03, November 2, 2004 Trustix Secure Linux Security Advisory, TSLSA-2004-0056, November 5, 2004 Mandrakelinux Security

				Update Advisory, MDKSA-2004:134, November 17,2004 Turbolinux Security Announcement, November 18, 2004 **SUSE Security Summary Report, SUSE-SR:2004:001, November 24, 2004**
Apple iCal 1.5.3	A vulnerability exists in the iCal calendar software due to a failure to warn an end user if the calendar contains an alarm, which could let a remote malicious user obtain/modify user information or execute arbitrary code. Upgrade available at: http://www.apple.com/ical/download/ There is no exploit code required.	Apple iCal Calendar Import Alarm Notification Failure CVE Name: CAN-2004-1021	Medium/ High (High if arbitrary code can be executed)	Apple Security Advisory, APPLE-SA-2004-11-22, November 22, 2004
Apple Safari Beta 2, 1.0-1.2.3	A Denial of Service vulnerability exists when an infinity JavaScript array sort operation is performed. No workaround or patch available at time of publishing. A Proof of Concept exploit has been published.	Apple Safari Web Browser Infinite Array Sort Denial of Service	Low	Bugtraq, November 25, 2004
Atari Atari800 1.3.1 & prior	Several buffer overflow vulnerabilities exist in the 'log.c' and 'rt-config.c' files due to insufficient boundary checks, which could let a malicious user execute arbitrary code with root privileges. The vendor reports that the vulnerability described in 'log.c' is fixed in versions after 2003-11-13, and that they are currently looking into the issue in 'rt-config.c'. An exploit script has been published.	Atari800 Emulator Multiple Buffer Overflows	High	Securiteam, November 25, 2004
energymech. net EnergyMech 2.99.79 & prior	A buffer overflow vulnerability exists when a remote authenticated malicious user submits a specially crafted 'ESAY' command. The impact was not specified. Update available at: http://www.energymech.net/download.html Currently we are not aware of any exploits for this vulnerability.	EnergyMech ESAY Command Buffer Overflow	Not Specified	SecurityTracker Alert ID, 1012360, November 30, 2004
GD Graphics Library gdlib 2.0.23, 2.0.26-2.0.28	A vulnerability exists in the 'gdImageCreateFromPngCtx()' function when processing PNG images due to insufficient sanity checking on size values, which could let a remote malicious user execute arbitrary code. OpenPKG: ftp://ftp.openpkg.org/release/ Ubuntu: http://security.ubuntu.com/ubuntu/pool/main/libg/libgd2/ Gentoo: http://security.gentoo.org/glsa/glsa-200411-08.xml Debian: http://security.debian.org/pool/updates/main/libg Fedora: http://download.fedora.redhat.com/pub/fedora/linux/core/updates/ Mandrake: http://www.mandrakesecure.net/en/ftp.php Trustix: http://http.trustix.org/pub/trustix/updates/ **SuSE: ftp://ftp.suse.com/pub/suse** An exploit script has been published.	GD Graphics Library Remote Integer Overflow CVE Name: CAN-2004-0990	High	Secunia Advisory, SA12996, October 28, 2004 Gentoo Linux Security Advisory, GLSA 200411-08, November 3, 2004 Ubuntu Security Notice, USN-21-1, November 9, 2004 Debian Security Advisories, DSA 589-1 & 591-1, November 9, 2004 Fedora Update Notifications, FEDORA-2004-411 & 412, November 11, 2004 Mandrakelinux Security Update Advisory, MDKSA-2004:132, November 15, 2004 Trustix Secure Linux Security Advisory, TSLSA-2004-0058, November 16, 2004 Ubuntu Security Notice, USN-25-1, November 16, 2004

				SUSE Security Summary Report, SUSE-SR:2004:001, November 24, 2004
GNU a2ps 4.13	A vulnerability exists in filenames due to insufficient validation of shell escape characters, which could let a malicious user execute arbitrary commands. FreeBSD: http://www.freebsd.org/cgi/cvsweb.cgi/~checkout~/ports/print/a2ps-letter/files/patch-select.c?rev=1.1&content-type=text/plain SuSE: ftp://ftp.suse.com/pub/suse/ Sun: http://sunsolve.sun.com/search/document.do?assetkey=1-26-57649-1&searchclause= **Mandrake:** **http://www.mandrakesecure.net/en/ftp.php** There is no exploit code required; however, a Proof of Concept exploit has been published.	GNU a2ps Command Injection	High	Securiteam, August 29, 2004 SUSE Security Announcement, SUSE-SA:2004:034, September 17, 2004 Sun(sm) Alert Notification, 57649, September 23, 2004 **Mandrakelinux Security Update Advisory, MDKSA-2004:140, November 26, 2004**
GNU InetUtils 1.4.2	A buffer overflow vulnerability exists in 'main.c' due to boundary errors when handling DNS responses, which could let a remote malicious user execute arbitrary code. **SuSE:** **ftp://ftp.suse.com/pub/suse** We are not aware of any exploits for this vulnerability.	GNU InetUtils TFTP Client Remote Buffer Overflow	High	Bugtraq, October 26, 2004 **SUSE Security Summary Report, SUSE-SR:2004:001, November 24, 2004**
ImageMagick ImageMagick 5.3.3, 5.4.3, 5.4.4.5, 5.4.7, 5.4.8 .2-1.1.0, 5.4.8, 5.5.3 .2-1.2.0, 5.5.6 .0-20030409, 5.5.7, 6.0, 6.0.1, 6.0.3-6.0.8	A buffer overflow vulnerability exists in the 'EXIF' parsing routine due to a boundary error, which could let a remote malicious user execute arbitrary code. Upgrades available at: http://sourceforge.net/project/showfiles.php?group_id=24099 Redhat: http://rhn.redhat.com/errata/RHSA-2004-480.html Ubuntu: http://security.ubuntu.com/ubuntu/pool/main/i/imagemagick/ Gentoo: http://security.gentoo.org/glsa/glsa-200411-11.xml Debian: http://security.debian.org/pool/updates/main/i/imagemagick/ SuSE: ftp://ftp.suse.com/pub/suse/i386/update/ Currently we are not aware of any exploits for this vulnerability.	ImageMagick Remote EXIF Parsing Buffer Overflow CVE Name: CAN-2004-0981	High	SecurityTracker Alert ID, 1011946, October 26, 2004 Gentoo Linux Security Advisory, GLSA 200411-11:01, November 6, 2004 Debian Security Advisory DSA 593-1, November 16, 2004 SUSE Security Announcement, SUSE-SA:2004:041, November 17, 2004 **SUSE Security Summary Report, USE-SR:2004:001, November 24, 2004**
Info-ZIP Zip 2.3	A buffer overflow vulnerability exists due to a boundary error when doing recursive compression of directories with 'zip,' which could let a remote malicious user execute arbitrary code. Ubuntu: http://security.ubuntu.com/ubuntu/pool/main/z/zip/ Fedora: http://download.fedora.redhat.com/pub/fedora/linux/core/updates/ Gentoo: http://security.gentoo.org/glsa/glsa-200411-16.xml **Mandrake:** **http://www.mandrakesecure.net/en/ftp.php** Currently we are not aware of any exploits for this vulnerability.	Info-ZIP Zip Remote Recursive Directory Compression Buffer Overflow CVE Name: CAN-2004-1010	High	Bugtraq, November 3, 2004 Ubuntu Security Notice, USN-18-1, November 5, 2004 Fedora Update Notification, FEDORA-2004-399 & FEDORA-2004-400, November 8 & 9, 2004 Gentoo Linux Security Advisory, GLSA 200411-16, November 9, 2004 **Mandrakelinux Security Update Advisory, MDKSA-2004:141, November 26, 2004**

ipcop.org IPCop 1.4.1, possibly older versions	A Cross-Site Scripting vulnerability exists in 'proxylog.dat' due to insufficient input validation, which could let a remote malicious user execute arbitrary HTML and script code. No workaround or patch available at time of publishing. A Proof of Concept exploit has been published.	IPCop 'proxylog.dat' Cross-Site Scripting	High	SecurityTracker Alert ID, 1012362, November 30, 2004
Jabber Software Foundation Jabber Server 2.0	Multiple buffer overflow vulnerabilities exists due to insufficient validation of user-supplied strings prior to copying them into finite process buffers, which could let a remote malicious user execute arbitrary code. No workaround or patch available at time of publishing. A Proof of Concept exploit has been published.	Jabber Server Multiple Remote Buffer Overflows CVE Name: CAN-2004-0953	High	Bugtraq, November 24, 2004
Mozilla.org Camino 0.7.0, 0.8	A Denial of Service vulnerability exists when the browser performs an infinite JavaScript array sort operation. No workaround or patch available at time of publishing. A Proof of Concept exploit has been published.	Mozilla Camino Web Browser Infinite Array Sort Denial of Service	Low	Bugtraq, November 25, 2004
Mozilla.org Bugzilla 2.4, 2.6, 2.8, 2.10, 2.12, 2.14-2.14.5, 2.16-2.16.5, 2.17-2.17.7, 2.18 rc1&rc2	Multiple vulnerabilities exist: a vulnerability exists in 'process_bug.cgi' when a specially crafted HTTP POST request to remove keywords from a bug is submitted, which could let a remote malicious user obtain sensitive information: a vulnerability exists when exporting bugs to XML, which could let a remote malicious user obtain sensitive information; and a vulnerability exists because various private attachment metadata is disclosed, which could let a remote malicious user see private attachments. Upgrades available at: http://www.bugzilla.org/download/ **Conectiva:** **ftp://atualizacoes.conectiva.com.br/** There is no exploit code required.	Mozilla Bugzilla Multiple Authentication Bypass& Information Disclosure	Medium	Bugzilla Security Advisory, October 24, 2004 **Conectiva Linux Security Announcement, CLA-2004:896, November 23, 2004**
Multiple Vendors Carnegie Mellon University Cyrus IMAP Server 2.1.7, 2.1.9, 2.1.10, 2.1.16, 2.2 .0 ALPHA, 2.2.1 BETA, 2.2.2 BETA, 2.2.3-2.2.8; Trustix Secure Enterprise Linux 2.0, Secure Linux 2.0-2.2; Ubuntu Linux 4.1 ppc, 4.1 ia64, 4.1 ia32	Multiple vulnerabilities exist: a buffer overflow vulnerability exists in the 'PROXY' and 'LOGIN' commands if the 'IMAPMAGICPLUS' option is enabled, which could let a remote malicious user execute arbitrary code; an input validation vulnerability exists in the argument parser for the 'PARTIAL' command, which could let a remote malicious user execute arbitrary code; an input validation vulnerability exists in the argument handler for the 'FETCH' command, which could let a remote malicious user execute arbitrary code; and a vulnerability exists in the handler for the 'APPEND' command, which could let a remote malicious user execute arbitrary code. Carnegie Mellon University: ftp://ftp.andrew.cmu.edu/pub/cyrus/ Debian: http://security.debian.org/pool/updates/main/c/cyrus-imapd/ Gentoo: http://security.gentoo.org/glsa/glsa-200411-34.xml Mandrake: http://www.mandrakesecure.net/en/ftp.php Trustix: http://http.trustix.org/pub/trustix/updates/ Ubuntu: http://security.ubuntu.com/ubuntu/pool/main/c/cyrus21-imapd/ Currently we are not aware of any exploits for these vulnerabilities.	Cyrus IMAPD Multiple Remote Vulnerabilities CVE Names: CAN-2004-1011 CAN-2004-1012 CAN-2004-1013	High	Securiteam, November 23, 2004 Debian Security Advisory, DSA 597-1, November 25, 2004 Gentoo Linux Security Advisory, GLSA 200411-34, November 25, 2004 Mandrakelinux Security Update Advisory, MDKSA-2004:139, November 26, 2004 Trustix Secure Linux Advisory, TSL-2004-0063. November 29,2 004
Multiple Vendors Carnegie Mellon University Cyrus IMAP Server 2.2.9 & prior	A buffer overflow vulnerability exists in the 'imap magic plus' support code, which could let a remote malicious user execute arbitrary code. Update available at: http://asg.web.cmu.edu/cyrus/download/ Gentoo: http://security.gentoo.org/glsa/glsa-200411-34.xml Mandrake: http://www.mandrakesecure.net/en/ftp.php Currently we are not aware of any exploits for this vulnerability.	Cyrus IMAP 'imap magic plus' Buffer Overflow CVE Name: CAN-2004-1015	High	Gentoo Linux Security Advisory, GLSA 200411-34, November 25, 2004 Mandrakelinux Security Update Advisory, MDKSA-2004:139, November 26, 2004

Multiple Vendors Gentoo Linux; Samba Samba 3.0-3.0.7	A remote Denial of Service vulnerability exists in 'ms_fnmatch()' function due to insufficient input validation. Patch available at: http://us4.samba.org/samba/ftp/patches/security/samba-3.0.7-CAN-2004-0930.patch Gentoo: http://security.gentoo.org/glsa/glsa-200411-21.xml Mandrake: http://www.mandrakesecure.net/en/ftp.php SuSE: ftp://ftp.suse.com/pub/suse/i386/update/ Ubuntu: http://security.ubuntu.com/ubuntu/pool/main/s/samba/ RedHat: http://rhn.redhat.com/errata/RHSA-2004-632.html Trustix: http://http.trustix.org/pub/trustix/updates/ **Conectiva:** **ftp://atualizacoes.conectiva.com.br/** **Fedora:** **http://download.fedora.redhat.com/pub/fedora/linux/core/updates/** There is no exploit code required.	Samba Remote Wild Card Denial of Service CVE Name: CAN-2004-0930	Low	SecurityFocus, November 15, 2004 Trustix Secure Linux Security Advisory, TSLSA-2004-0058, November 16, 2004 RedHat Security Advisory, RHSA-2004:632-17, November 16, 2004 **Conectiva Linux Security Announcement, CLA-2004:899, November 25, 2004** **Fedora Update Notifications, FEDORA-2004-459 & 460, November 29, 2004**
Multiple Vendors Samba 3.0 - 3.0.7; RedHat Advanced Workstation for the Itanium Processor 2.1, IA64, Desktop 3.0, Enterprise Linux WS 3, WS 2.1 IA64, 2.1, ES 3, 2.1 IA64, 2.1, AS 3, 2.1 IA64, 2.1; Ubuntu Linux 4.1 ppc, ia64, ia32	A buffer overflow vulnerability exists in the 'QFILEPATHINFO' request handler when constructing 'TRANSACT2_QFILEPATHINFO' responses, which could let a remote malicious user execute arbitrary code. Update available at: http://www.samba.org/samba/download/ Mandrake: http://www.mandrakesecure.net/en/ftp.php SuSE: ftp://ftp.suse.com/pub/suse/ Trustix: ftp://ftp.trustix.org/pub/trustix/updates/ Ubuntu: Ubuntu Upgrade samba-doc 3.0.7-1ubuntu6.2 all.deb **Conectiva:** **ftp://atualizacoes.conectiva.com.br/** **Fedora:** **http://download.fedora.redhat.com/pub/fedora/linux/core/updates/** Currently we are not aware of any exploits for this vulnerability.	Samba 'QFILEPATHINFO' Buffer Overflow CVE Name: CAN-2004-0882	High	e-matters GmbH Security Advisory, November 14, 2004 SuSE Security Announcement, SUSE-SA:2004:040, November 15, 2004 Trustix Secure Linux Security Advisory, TSLSA-2004-0058, November 16, 2004 Ubuntu Security Notice, USN-29-1, November 18, 2004 Mandrakelinux Security Update Advisory, MDKSA-2004:136, November 19, 2004 US-CERT Vulnerability Note VU#457622, November 19, 2004 **Conectiva Linux Security Announcement, CLA-2004:899, November 25, 2004** **Fedora Update Notifications, FEDORA-2004-459 & 460, November 29, 2004**

Multiple Vendors Gentoo Linux; RedHat Fedora Core3, Core2; SuSE Linux 8.1, 8.2, 9.0-9.2, Desktop 1.0, Enterprise Server 9, 8, Novell Linux Desktop 1.0; X.org X11R6 6.7 .0, 6.8, 6.8.1; XFree86 X11R6 3.3, 3.3.2-3.3.6, 4.0-4.0.3, 4.1 .0, 4.1 -12, 4.1 -11, 4.2 .0, 4.2.1 Errata, 4.2.1 4.3 .0	Multiple vulnerabilities exist due to integer overflows, memory access errors, input validation errors, and logic errors, which could let a remote malicious user execute arbitrary code, obtain sensitive information or cause a Denial of Service. Fedora: http://download.fedora.redhat.com/pub/fedora/linux/core/updates Gentoo: http://security.gentoo.org/glsa/glsa-200411-28.xml SuSE: ftp://ftp.suse.com/pub/suse X.org: http://www.x.org/pub/ **Mandrake:** **http://www.mandrakesecure.net/en/ftp.php** Currently we are not aware of any exploits for these vulnerabilities	LibXPM Multiple Vulnerabilities CVE Name: CAN-2004-0914	Low/ Medium/ High (Low if a DoS; Medium if sensitive information can be obtained; and High if arbitrary code can be executed)	X.Org Foundation Security Advisory, November 17, 2004 Fedora Update Notifications, FEDORA-2004-433 & 434, November 17 & 18, 2004 SUSE Security Announcement, SUSE-SA:2004:041, November 17, 2004 Gentoo Linux Security Advisory, GLSA 200411-28, November 19, 2004 **Mandrakelinux Security Update Advisories, MDKSA-2004:137 & 138, November 23, 2004**
Multiple Vendors Linux kernel 2.6.x, 2.4.x	Two vulnerabilities exist: a Denial of Service vulnerability exists via a specially crafted 'a.out' binary; and a vulnerability exists due to a race condition in the memory management, which could let a malicious user obtain sensitive information. No workaround or patch available at time of publishing. Currently we are not aware of any exploits for these vulnerabilities.	Linux Kernel Local DoS & Memory Content Disclosure	Low/ Medium (Medium if sensitive information can be obtained)	Secunia Advisory, SA13308, November 25, 2004
Multiple Vendors Linux Kernel 2.4.28 & prior	A vulnerability exists due to improper serialization of datagrams, which could let a malicious user obtain elevated privileges. Update available at: http://linux.bkbits.net:8080/linux-2.4/cset@4199284dnTPrPLR-yhP_rOBHXJlltA Currently we are not aware of any exploits for this vulnerability.	Linux Kernel Datagram Serialization CVE Name: CAN-2004-1068	Medium	SecurityTracker Alert ID, 1012363, November 30, 2004
Multiple Vendors Linux Kernel 2.4-2.4.27, 2.6-2.6.8	Multiple vulnerabilities exist due to various errors in the 'load_elf_binary' function of the 'binfmt_elf.c' file, which could let a malicious user obtain elevated privileges and potentially execute arbitrary code. Patch available at: http://linux.bkbits.net:8080/linux-2.6/gnupatch@41925edcVccsXZXObG444GFvEJ94GQ Trustix: http://http.trustix.org/pub/trustix/updates/ **Fedora:** **http://download.fedora.redhat.com/pub/fedora/linux/core/updates/** Proofs of Concept exploit scripts have been published.	Linux Kernel BINFMT_ELF Loader Multiple Vulnerabilities	Medium/ High (High if arbitrary code can be executed)	Bugtraq, November 11, 2004 **Fedora Update Notifications, FEDORA-2004-450 & 451, November 23, 2004**
Multiple Vendors Linux Kernel 2.4-2.4.27, 2.6-2.6.9; Trustix Secure Enterprise Linux 2.0, Secure Linux 1.5, 2.0-2.2; Ubuntu Linux 4.1 ppc, 4.1 ia64, 4.1 ia32	Multiple remote Denial of Service vulnerabilities exist in the SMB filesystem (SMBFS) implementation due to various errors when handling server responses. This could also possibly lead to the execution of arbitrary code. Upgrades available at: http://kernel.org/pub/linux/kernel/v2.4/linux-2.4.28.tar.bz2 Trustix: ftp://ftp.trustix.org/pub/trustix/updates/ Ubuntu: http://security.ubuntu.com/ubuntu/pool/main/l/ **Fedora:** **http://download.fedora.redhat.com/pub/fedora/linux/core/updates/** Currently we are not aware of any exploits for these vulnerabilities	Linux Kernel smbfs Filesystem Memory Errors Remote Denial of Service CVE Names: CAN-2004-0883 CAN-2004-0949	Low/High (High if arbitrary code can be executed)	e-matters GmbH Security Advisory, November 11, 2004 **Fedora Update Notifications, FEDORA-2004-450 & 451, November 23, 2004**

MySQL AB MySQL 3.23.49, 4.0.20	A vulnerability exists in the 'mysqlhotcopy' script due to predictable files names of temporary files, which could let a malicious user obtain elevated privileges. Debian: http://security.debian.org/pool/updates/main/m/ Gentoo: http://security.gentoo.org/glsa/glsa-200409-02.xml SuSE: ftp://ftp.suse.com/pub/suse/ RedHat: http://rhn.redhat.com/errata/RHSA-2004-569.html OpenPKG: ftp://ftp.openpkg.org/release/ Mandrake: http://www.mandrakesoft.com/security/advisories There is no exploit code required.	MySQL 'Mysqlhotcopy' Script Elevated Privileges CVE Name: CAN-2004-0457	Medium	Debian Security Advisory, DSA 540-1, August 18, 2004 Gentoo Linux Security Advisory GLSA 200409-02, September 1, 2004 SUSE Security Announcement, SUSE-SA:2004:030, September 6, 2004 RedHat Security Advisory, ,RHSA-2004:569-16, October 20, 2004 Mandrakelinux Security Update Advisory, MDKSA-2004:119, November 1, 2004 **SUSE Security Summary Report, USE-SR:2004:001, November 24, 2004**
MySQL AB MySQL 3.x, 4.x	Two vulnerabilities exist: a vulnerability exists due to an error in 'ALTER TABLE ... RENAME' operations because the 'CREATE/INSERT' rights of old tables are checked, which potentially could let a remote malicious user bypass security restrictions; and a remote Denial of Service vulnerability exists when multiple threads issue 'alter' commands against 'merge' tables to modify the 'union.' Updates available at: http://dev.mysql.com/downloads/mysql/ Debian: http://security.debian.org/pool/updates/main/m/mysql Trustix: http://http.trustix.org/pub/trustix/updates/ Mandrake: http://www.mandrakesoft.com/security/advisories Conectiva: ftp://atualizacoes.conectiva.com.br/ **Ubuntu:** **http://security.ubuntu.com/ubuntu/pool/main/m/mysql-dfsg/** **SuSE:** **ftp://ftp.suse.com/pub/suse** We are not aware of any exploits for these vulnerabilities.	MySQL Security Restriction Bypass & Remote Denial of Service CVE Names: CAN-2004-0835 CAN-2004-0837	Low/ Medium (Low if a DoS; and Medium if security restrictions can be bypassed)	Secunia Advisory, SA12783, October 11, 2004 Trustix Secure Linux Security Advisory, TSLSA-2004-0054, October 15, 2004 Mandrakelinux Security Update Advisory, MDKSA-2004:119, November 1, 2004 Conectiva Linux Security Announcement, CLA-2004:892, November 18, 2004 **Ubuntu Security Notice, USN-32-1, November 25, 2004** **SUSE Security Summary Report, SUSE-SR:2004:001, November 24, 2004**
phpBB Group phpBB 2.0.0-2.0.10	A vulnerability exists in the 'urldecode' function due to insufficient input validation, which could let a remote malicious user execute arbitrary PHP script. No workaround or patch available at time of publishing. **An exploit script has been published.**	PHPBB Remote URLDecode Input Validation	High	Bugtraq, November 13, 2004 **SecurityFocus, November 23, 2004**
PHPNews PHPNews 1.2.3	A vulnerability exists in 'sendtofriend.php' due to insufficient sanitization of the 'mid' parameter, which could let a remote malicious user manipulate data. Upgrade available at: http://prdownloads.sourceforge.net/newsphp/phpnews_1-2-4.zip?download There is no exploit code required.	PHPNews SQL Injection	Medium	Secunia Advisory, SA13300, November 24, 2004
phpWebSite Development Team phpWebsite 0.7.3, 0.8.2,	A vulnerability exists in the 'index.php' script due to insufficient validation of user-supplied input in several parameters, which could let a remote malicious user execute arbitrary HTML and script code. Patches available at: http://phpwebsite.appstate.edu/downloads/	phpWebSite HTTP Response Splitting	High	Secunia Advisory, SA13172, November 12, 2004 **Gentoo Linux Security Advisory, GLSA**

0.8.3, 0.9.3, -1-4	security/phpwebsite-core-security-patch2.tar.gz **Gentoo:** **http://security.gentoo.org/glsa/glsa-200411-35.xml** An exploit script is not required; however, a Proof of Concept exploit has been published.			**200411-35:02, November 26, 2004**
ProZIlla ProZilla Download Accelerator 1.0 x, 1.3.0-1.3.4, 1.3.5.2, 1.3.5 .1, 1.3.5, 1.3.6	Multiple buffer overflow vulnerabilities exist due to boundary errors in the communication handling, which could let a remote malicious user execute arbitrary code. Gentoo: http://security.gentoo.org/glsa/glsa-200411-31.xml Exploit scripts have been published.	ProZilla Multiple Remote Buffer Overflow	High	Secunia Advisory, SA13294, November 24, 2004
Roaring Penguin Software MIMEDefang 2.4, 2.14, 2.20, 2.21, 2.38, 2.39, 2.41-4.47	Multiple vulnerabilities exists due to insufficient validation of I/O operations in 'mimedefang.pl.in' and an unspecified input validation error exists in 'mimedefang.c.' The impact was not specified. Upgrades available at: http://www.mimedefang.org/static/mimedefang-2.48.tar.gz Gentoo: http://security.gentoo.org/glsa/glsa-200411-06.xml Mandrake: http://www.mandrakesecure.net/en/ftp.php **SuSE:** **ftp://ftp.suse.com/pub/suse** We are not aware of any exploits for these vulnerabilities.	Roaring Penguin Software MIMEDefang Multiple Vulnerabilities	Not Specified	SecurityTracker Alert ID, 1011996, October 29, 2004 **SUSE Security Summary Report, SUSE-SR:2004:001, November 24, 2004**
The BNC Project BNC 2.2.4, 2.4.6, 2.4.8, 2.6, 2.6.2, 2.8.8, 2.8.9	A buffer overflow vulnerability exists in ' getnickuserhost' when a malformed IRC server response is handled by the proxy, which could let a remote malicious user execute arbitrary code. Upgrades available at: http://www.gotbnc.com/files/bnc2.9.1.tar.gz Gentoo: http://security.gentoo.org/glsa/glsa-200411-24.xml **Debian:** **http://security.debian.org/pool/updates/main/b/bnc/** Currently we are not aware of any exploits for this vulnerability.	BNC Remote Buffer Overflow CVE Name: CAN-2004-1052	High	LSS Security Advisory #LSS-2004-11-3, November 10, 2004 Gentoo Linux Security Advisory, GLSA 200411-24, November 16, 2004 **Debian Security Advisory, DSA 595-1, November 24, 2004**
Todd Miller Sudo 1.5.6-1.5.9, 1.6-1.6.8	A vulnerability exists due to an error in the environment cleaning, which could let a malicious user execute arbitrary commands. Patch available at: http://www.courtesan.com/sudo/download.html Mandrake: http://www.mandrakesecure.net/en/ftp.php Trustix: http://http.trustix.org/pub/trustix/updates/ Ubuntu: http://security.ubuntu.com/ubuntu/pool/main/s/sudo/ **Debian:** **http://security.debian.org/pool/updates/main/s/sudo/** There is no exploit code required.	Sudo Restricted Command Execution Bypass	High	Secunia Advisory, SA13199, November 15, 2004 Mandrakelinux Security Update Advisory, MDKSA-2004:133, November 15, 2004 Trustix Secure Linux Security Advisories, TSLSA-2004-0058 & 061, November 16 & 19, 2004 Ubuntu Security Notice, USN-28-1, November 17, 2004 **Debian Security Advisory, DSA 596-1, November 24, 2004**
TWiki TWiki 20030201	A vulnerability exists in 'Search.pn' due to an input validation error when handling search requests, which could let a remote malicious user execute arbitrary commands. Hotfix available at: http://twiki.org/cgi-bin/view/Codev/SecurityAlertExecuteCommandsWithSearch **Gentoo:** **http://security.gentoo.org/**	TWiki Search Shell Metacharacter Remote Arbitrary Command Execution CVE Name: CAN-2004-1037	High	Securiteam, November 15, 2004 PacketStorm, November 20, 2004 **Gentoo Linux Security Advisory, GLSA 200411-33, November 24, 2004**

	glsa/glsa-200411-33.xml An exploit script has been published.			
wmFrog Weather Monitor 0.1.6	A vulnerability exists due to insecure creation of temporary files, which could let a malicious user overwrite arbitrary files on the system. No workaround or patch available at time of publishing. There is no exploit code required.	WMFrog Weather Monitor Insecure Temporary Files	Medium	Secunia Advisory, SA13259, November 24, 2004
xinehq.de xine 0.5.2 - 0.5.x; 0.9.x; 1-alpha.x; 1-beta.x; 1-rc - 1-rc5	Multiple vulnerabilities exist: a buffer overflow vulnerability exists in the DVD subpicture component, which could let a remote malicious user execute arbitrary code; a buffer overflow vulnerability exists in the VideoCD functionality when reading ISO disk labels, which could let a remote malicious user execute arbitrary code; and a buffer overflow vulnerability exists when handling text subtitles, which could let a remote malicious user execute arbitrary code. Upgrades available at: http://prdownloads.sourceforge.net/xine/xine-lib-1-rc6a.tar.gz?download Gentoo: http://security.gentoo.org/glsa/glsa-200409-30.xml Mandrake: http://www.mandrakesecure.net/en/ftp.php **SuSE:** **ftp://ftp.suse.com/pub/suse** We are not aware of any exploits for these vulnerabilities.	Xine-lib Multiple Buffer Overflows	High	Secunia Advisory, SA12602 September 20, 2004 Gentoo Linux Security Advisory, GLSA 200409-30, September 22, 2004 Mandrakelinux Security Update Advisory, MDKSA-2004:105, October 6, 2004 **SUSE Security Summary Report, SUSE-SR:2004:001, November 24, 2004**
Yard RADIUS Yard RADIUS 1.0 pre13-pre15, 1.0.16-1.0.20	A buffer overflow vulnerability exists in the 'process_menu()' function and the 'calc_acctreq()' function, which could let a remote malicious user execute arbitrary code. Upgrades available at: http://sourceforge.net/project/showfiles.php?group_id=10594&package_id=10142 Debian: http://security.debian.org/pool/updates/main/y/yardradius/ Currently we are not aware of any exploits for this vulnerability.	Yard Radius Remote Buffer Overflows CVE Name: CAN-2004-0987	High	Debian Security Advisory, DSA 598-1, November 25, 2004

[back to top]

Multiple Operating Systems - Windows / UNIX / Linux / Other

Vendor & Software Name	Vulnerability - Impact Patches - Workarounds Attacks Scripts	Common Name	Risk	Source
F-Secure Internet Security 2004, Anti-Virus 2004, 2005, Anti-Virus Client Security 5.50, 5.52, 5.55, Anti-Virus for Linux Gateways 4.51, 4.52, 4.61, Anti-Virus for Linux Servers 4.51, 4.52, 4.61, Anti-Virus for Linux Workstations 4.51, 4.52, Anti-Virus for MIMEsweeper 5.41, 5.42, 5.50, Anti-Virus for MS Exchange 6.0 1, 6.2, 6.3, 6.21 6.30 Service Release 1, 6.31, Anti-Virus for Samba Servers 4.60, Anti-Virus for Windows Servers 5.41, 5.42, 5.50, Anti-Virus for Workstations 5.41, 5.42, 5.43, Anti-Virus Linux Client Security 5.0, Anti-Virus Linux Server Security 5.0, F-Secure	A vulnerability exists due to an error when parsing '.zip' archives, which could let a remote malicious user bypass certain scanning functionality that results in a false sense of security and the execution of malicious applications. Hotfixes available at: http://support.f-secure.com/enu/corporate/downloads/hotfixes Currently we are not aware of any exploits for this vulnerability.	F-Secure Anti-Virus ZIP Archive Scanner Bypass	High	F-Secure Security Bulletin FSC-2004-3, November 23, 2004

for Firewalls 6.20, Internet Gatekeeper 6.3, 6.4, 6.31, 6.32, 6.41, Internet Gatekeeper for Linux 2.6, Internet Security 2005, Personal Express 4.5, 4.6, 4.7, 5.0				
Gearbox Software Halo Combat Evolved 1.2, 1.4, 1.5, 1.31	A remote Denial of Service vulnerability exists when a malicious user submits a specially crafted packet. The vendor has issued a fixed version (1.06). An exploit script has been published.	Gearbox Software Halo Game Client Remote Denial of Service	Low	Securiteam, November 23, 2004
Inkra Networks Corporation 1504GX VSM 2.1.4.b003	A remote Denial of Service vulnerability exists due to insufficient validation of IP options. **The vendor has released an update to address this vulnerability. Customers are advised to contact the vendor for further information in regard to obtaining and applying an appropriate patch.** There is no exploit code required; however, Proof of Concept exploit has been published.	Inkra 1504GX Remote Denial of Service	Low	Secunia Advisory, SA12538, September 17, 2004 **SecurityFocus, November 23, 2004**
jspwiki.org JSPWiki 2.1.120, 2.1.121, 2.1.122	A Cross-Site Scripting vulnerability exists in 'Search.jsp' due to insufficient sanitization of the 'query' parameter, which could let a remote malicious user execute arbitrary HTML and script code. Upgrades available at: http://www.ecyrd.com/~jalkanen/JSPWiki/nightly/JSPWiki-latest.zip A Proof of Concept exploit has been published.	JSPWiki Cross-Site Scripting	High	STG Security Advisory, SSA-20041122-11, November 24, 2004
KorWeblog KorWeblog 1.6.2-cvs	A vulnerability exists in 'viewimg.php' due to insufficient verification of the 'path' parameter before being used to list directories inside the web root, which could let a remote malicious user obtain sensitive information. No workaround or patch available at time of publishing. A Proof of Concept exploit has been published.	KorWeblog Remote Directory Listing	Medium	STG Security Advisory, SSA-20041122-10, November 24, 2004
Liferay Enterprise Portal version 2.1.1 & prior	Almost all fields that take input from the user's browser are prone to XSS attacks. Inadequate filtering makes it easy for a malicious user to cause the victim's browser to execute script code. **Upgrade available at:** **http://prdownloads.sourceforge.net/lportal/liferay-ep-2.2.0-src.zip?download** Currently we are not aware of any exploits for this vulnerability.	Liferay Cross Site Scripting	High	Securiteam, May 24, 2004 **Bugtraq, November 25, 2004**
Mozilla.org Mozilla Browser M16, M15, 0.8, 0.9.2 .1, 0.9.2-0.9.9, 0.9.35, 0.9.48, 1.0, RC1, 1.0.1, 1.0.2, 1.1, Beta, Alpha, 1.2, Beta, Alpha, 1.2.1, 1.3, 1.3.1, 1.4 b, 1.4 a, 1.4, 1.4.1, 1.4.2, 1.5, 1.5.1, 1.6, 1.7, alpha, beta, rc1-rc3, 1.7.1-1.7.3, 1.8 Alpha 1-Alpha 4	A Denial of Service vulnerability exists when the browser performs an infinite JavaScript array sort operation. No workaround or patch available at time of publishing. A Proof of Concept exploit has been published.	Mozilla Browser Infinite Array Sort Denial of Service	Low	Bugtraq, November 25, 2004
Nuked-Klan Nuked-Klan 1.2 beta, 1.2, 1.3 beta, 1.3, 1.4, 1.5 SP2, 1.5	A Cross-Site Scripting vulnerability exists in the 'submit URI link' function due to insufficient input validation, which could let a remote malicious user execute arbitrary HTML and script code. No workaround or patch available at time of publishing. A Proof of Concept exploit has been published.	NuKed-Klan Cross-Site Scripting	High	SecurityTracker Alert ID, 1012305, November 23, 2004
opendchub.sourceforge.net Open DC Hub Direct Connect Peer-to-peer Client 0.7.14	A buffer overflow vulnerability exists in the 'RedirectAll' command due to a boundary error, which could let a remote malicious user execute arbitrary code. Gentoo: http://security.gentoo.org/glsa/glsa-200411-37.xml A Proof of Concept exploit script has been published.	Open DC Hub Remote Buffer Overflow	High	Gentoo Linux Security Advisory, GLSA 200411-37, November 29, 2004

Opera Software Opera Web Browser 5.0 2 win32, 5.0 Mac, 5.0 Linux, 5.1 0-5.12 win32, 5.1, 6.0 win32, 6.0 6, 6.0.6win32, 6.0, 6.0.1 win32, 6.0.1 linux, 6.0.1, 6.0.2 win32, 6.0.2 linux, 6.0.3 win32, 6.0.3 linux, 6.0.4 win32, 6.0.5 win32, 6.10 linux, 7.0 win32 Beta 1&2, 7.0 win32, 7.03win32, 7.0 2win32, 7.0 1win32, 7.10, 7.11 j, 7.11 b, 7.11, 7.20 Beta 1 build 2981, 7.20-7.23, 7.50-7.54	A remote Denial of Service vulnerability exists when the browser performs an infinite JavaScript array sort operation. No workaround or patch available at time of publishing. A Proof of Concept exploit has been published.	Opera Web Browser Infinite Array Sort Remote Denial of Service	Low	Bugtraq, November 25, 2004
phpBB Group phpBB 1.0 .0, 1.2 .0, 1.2.1, 1.4 .0-1.4.2, 1.4.4, 2.0 .0, rc1-rc4, Beta 1, 2.0.1-2.0.10	A vulnerability exists in the 'Cash_Mod' module due to insufficient verification of the input passed to the 'phpbb_root_path' parameter, which could let a remote malicious user execute arbitrary code. Upgrades available at: http://www.phpbb.com/phpBB/catdb.php?mode=download&id=539420 **Gentoo: http://security.gentoo.org/glsa/glsa-200411-32.xml** There is no exploit code required; however, a Proof of Concept exploit script has been published.	PHPBB Admin_cash.PHP Remote PHP File Include	High	Secunia Advisory ID, SA1324, November 19, 2004 **Gentoo Security Advisory, GLSA 200411-32, November 24, 2004**
phpBB Group phpBB 2.0.0-2.0.9	Multiple vulnerabilities exist: a vulnerability exists in 'viewtopic.php' due to insufficient sanitization of the 'highlight' parameter, which could let a malicious user obtain sensitive information or execute arbitrary code; a vulnerability exists due to insufficient sanitization of input passed to the username handling, which could let a remote malicious user execute arbitrary HTML or script code; and a vulnerability exists due to insufficient sanitization of input passed to the username handling before being used in an SQL query, which could let a malicious user execute arbitrary code. Upgrades available at: http://www.phpbb.com/downloads.php **Gentoo: http://security.gentoo.org/glsa/glsa-200411-32.xml** There is no exploit code required; however, a Proof of Concept exploit script has been published.	PHPBB Login Form Multiple Input Validation	High	SECUNIA ADVISORY ID: SA13239, November 19, 2004 **Gentoo Linux Security Advisory, GLSA 200411-32, November 24, 2004**
phpcms.de phpCMS 1.1.9, 1.2 .0, 1.2.1	A Cross-Site Scripting vulnerability exists when configured with one or both of the 'STEALTH' or 'STEALTH_SECURE' modes disabled due to insufficient sanitization of user-supplied input, which could let a remote malicious user execute arbitrary HTML and script code. Upgrades available at: http://prdownloads.sourceforge.net/phpcms/phpcms-1.2.1pl1.tar.gz?download A Proof of Concept exploit has been published.	PHPCMS Cross-Site Scripting	High	Bugtraq, November 26, 2004
phpkit.de PHPKIT 1.6.1, 1.6.03, 1.6.02	Several vulnerabilities exist: a Cross-Site Scripting vulnerability exists in 'popup.php' due to insufficient sanitization of the 'img' parameter, which could let a remote malicious user execute arbitrary HTML and script code; and a vulnerability exists in 'include.php' due to insufficient sanitization of the 'id' parameter, which could let a remote malicious user manipulate SQL queries. No workaround or patch available at time of publishing. Proofs of Concept exploits have been published.	PHPKIT Multiple Input Validation	Medium/ High (High if arbitrary code can be executed)	Bugtraq, November 22, 2004
Plain Black Software WebGUI 6.2-6.2.8	A vulnerability exists due to an unspecified error in the 'user profile.' The impact was not specified. Upgrades available at: http://sourceforge.net/project/showfiles.php?group_id=51417 Currently we are not aware of any exploits for this vulnerability.	Plain Black Software WebGUI 'User profile'	Not Specified	Security Focus, November 22, 2004

Raven Software Soldier Of Fortune 2 1.03, 21.0 2	A buffer overflow vulnerability exists when a remote malicious user submits a specially crafted query (to a client), which could cause a Denial of Service. No workaround or patch available at time of publishing. A Proof of Concept exploit script has been published.	Soldier Of Fortune 2 Buffer Overflow Remote Denial of Service	Low	SecurityTracker Alert ID, 1012316, November 24, 2004
Sun Microsystems, Inc. Sun JRE (Linux Production Release)1.2.2 _010-1.2.2_015, 1.2.2 _003-1.2.2_007, 1.2.2, 1.3 .0-1.3.0_05, 1.3.1-1.3.1 _03, 1.3.1 _05-1.3.1 _09, 1.4, 1.4 .0_02-1.4 .0_04, 1.4.1-1.4.1_03, 1.4.2-1.4.2 _06, JRE (Solaris Production Release) 1.1.6, 1.1.7 B, 1.1.8, 1.1.8 _009, 1.1.8 _010, 1.1.8 _12-1.1.8_14, 1.1.8 _009, 1.1.8, 1.2, 1.2.1, 1.2.2_11, 1.2.2 _07, 1.2.2 _05a, .2.2 _010-2.2._014, 1.2.2, 1.3.0_05, 1.3 .0_02, 1.3, 1.3.1 _01-1.3.1 _09, 1.4.0_011.4.0_04, 1.4, 1.4.1 _03, 1.4.1 _02, 1.4.1 _01, .4.1, 1.4.2_01-1.4.2 _06, 1.4.2, Windows Production Release) 1.1.6 _009, 1.1.7 B_007, 1.1.8 _009, 1.1.8 _008, 1.1.8 _007, 1.1.8 _005, 1.1.8, 1.2, 1.2.1, 1.2.2 _12, 1.2.2_015, 1.2.2 _014, 1.2.2 _013, 1.2.2 _011, 1.2.2 _010, 1.2.2 _007, 1.2.2, 1.3 .0_05, 1.30_04, 1.3 .0_02, 1.3, 1.3.1 _01-1.3.1 _09, 1.4.0_01-1.4.0_04, 1.4, 1.4.1 _07, 1.4.1 _03, 1.4.1 _02, 1.4.1 _01, 1.4.1, 1.4.2 _01-1.4.2_06, 1.4.2	A vulnerability exists because it is possible to cause a previous version of a plug-in, that is known to be prone to security vulnerabilities, to be loaded in lieu of a more recent version that has been patched, which could result in a false sense of security. No workaround or patch available at time of publishing. An exploit script is not required; however, a Proof of Concept exploit has been published.	Sun Java Applet Invocation Version Specification	Medium	SecurityFocus, November 25, 2004
Sun Microsystems, Inc. Sun Java JRE 1.3.x, 1.4.x, Sun Java SDK 1.3.x, 1.4.x; **Conectiva Linux 10.0**	A vulnerability exists due to a design error because untrusted applets for some private and restricted classes used internally can create and transfer objects, which could let a remote malicious user turn off the Java security manager and disable the sandbox restrictions for untrusted applets. Updates available at: http://sunsolve.sun.com/search/document.do?assetkey=1-26-57591-1 **Conectiva:** **ftp://atualizacoes.conectiva.com.br/10/** Currently we are not aware of any exploits for this vulnerability.	Sun Java Plug-in Sandbox Security Bypass CVE Name: CAN-2004-1029	Medium	Sun(sm) Alert Notification, 57591, November 22, 2004 US-CERT Vulnerability Note, VU#760344, November 23, 2004 **Conectiva Linux Security Announcement, CLA-2004:900, November 26, 2004**

YaBB YaBB 1 Gold Release, SP 1, SP 1.2, SP 1.3-1.3.2, YaBB 1.40, 1.41, 9.1.2000, 9.11.2000	A vulnerability exists due to insufficient sanitization of 'shadow' tags, which could let a malicious user execute arbitrary code. Upgrades available at: http://www.yabbforum.com/downloads.php An exploit script is not required.	YaBB Shadow BBCode Tag JavaScript Injection	High	Secunia Advisory, SA13319, November 26, 2004
ZyXEL Communications Corp. Prestige 645R-A1, 650H, 650HW, 650HW-31, 650R, ZyNOS V3.40(ES.5), IS.5, IS.3, 3.40	A vulnerability exists due to a failure to restrict access to a configuration page that is part of the remote administration service, which could let a remote malicious user reset the configuration. No workaround or patch available at time of publishing. A Proof of Concept exploit has been published.	ZyXEL Prestige Router HTTP Remote Administration Configuration Reset	Medium	Bugtraq, November 21, 2004

Recent Exploit Scripts/Techniques

The table below contains a sample of exploit scripts and "how to" guides identified during this period. The "Workaround or Patch Available" column indicates if vendors, security vulnerability listservs, or Computer Emergency Response Teams (CERTs) have published workarounds or patches.

Note: At times, scripts/techniques may contain names or content that may be considered offensive.

Date of Script (Reverse Chronological Order)	Script name	Workaround or Patch Available	Script Description
November 26, 2004	101_mEna.c	No	Script that exploits the MailEnable IMAP Service Multiple Remote Pre-Authentication Buffer Overflow vulnerabilities.
November 26, 2004	atari800.c	Yes	Exploit for the Atari800 Emulator Multiple Local Buffer Overflow vulnerabilities.
November 24, 2004	evil_server.pl prozillaBufferOverflowExploitSerkanAkpolat.c proz_ex.c	Yes	Scripts that exploit the ProZilla Multiple Remote Buffer Overflow vulnerabilities.
November 24, 2004	openDCHubBufferOverflowPOC.java	Yes	A Proof of Concept exploit for the Open DC Hub Remote Buffer Overflow vulnerability.
November 24, 2004	sof2boom.zip	No	A Proof of Concept exploit for the Soldier Of Fortune 2 Buffer Overflow Remote Denial of Service vulnerability.
November 24, 2004	swbfp.zip	No	Exploit for the LucasArts Star Wars Battlefront Game Server Remote Denials of Service vulnerabilities.
November 24, 2004	winAmpIN_CDDALibExploit.c	Yes	Scripts that exploit the Nullsoft Winamp 'IN_CDDA.dll' Buffer Overflow vulnerability.
November 23, 2004	coffeeCupFTPBufferOverflowExpl.c	No	Script that exploits the CoffeeCup Direct/Free FTP ActiveX Component Remote Buffer Overflow vulnerability.
November 23, 2004	haloCboom.zip	Yes	Exploit for the Gearbox Software Halo Game Client Remote Denial of Service vulnerability.
November 23, 2004	phpBBCodeExecExploitRUSH.pl	No	Exploit for the PHPBB Remote URLDecode Input Validation vulnerability.
November 23, 2004	WodFtpDLXBufferOverflowExpl.c	Yes	Script that exploits the WeOnlyDo! wodFtpDLX ActiveX Component Remote Buffer Overflow vulnerability.

[back to top]

Trends

- Microsoft is clamping down on software pirates in the UK after discovering that a large volume of high quality counterfeit versions of Windows XP. Kicking off its Windows XP Counterfeit Project, the software giant has invited "anyone unsure as to the legitimacy of their Windows XP software" to submit their products for analysis. For more information see: http://www.vnunet.com/news/1159640.
- Computer criminals are making phishing more potent by automating attacks. Anti-Phishing Working Group (APWG) analysts suspect fraudsters are using automated tools and botnets to ramp up attacks. It estimates attacks grew by an average of 36 per cent a month between July and October. The US is home to the majority of these baiting sites, hosting 29 per cent of those reported to the APWG in October, a slight decrease over the month. China, Korea, and Russia are next on the list with 16 per cent, nine per cent, and eight per cent respectively of the total sites hosted. For more information, see APWG's report, jointly written by security researchers at Websense and Tumbleweed Communications, at: http://www.antiphishing.org/APWG_Phishing_Activity_Report-Oct2004.pdf

[back to top]

Viruses/Trojans

Top Ten Virus Threats

A list of high threat viruses, as reported to various anti-virus vendors and virus incident reporting organizations, has been ranked and categorized in the table below. For the purposes of collecting and collating data, infections involving multiple systems at a single location are considered a single infection. It is therefore possible that a virus has infected hundreds of machines but has only been counted once. With the number of viruses that appear each month, it is possible that a new virus will become widely distributed before the next edition of this publication. To limit the possibility of infection, readers are reminded to update their anti-virus packages as soon as updates become available. The table lists the viruses by ranking (number of sites affected), common virus name, type of virus code (i.e., boot, file, macro, multi-partite, script), trends (based on number of infections reported since last week), and approximate date first found.

Rank	Common Name	Type of Code	Trends	Date
1	Netsky-P	Win32 Worm	Stable	March 2004
2	Netsky-Z	Win32 Worm	Stable	April 2004
3	Netsky-B	Win32 Worm	Stable	March 2004
4	Zafi-B	Win32 Worm	Stable	June 2004
5	Bagle-AA	Win32 Worm	Stable	April 2004
6	Netsky-B	Win32 Worm	Stable	February 2004
7	Bagle-AT	Win32 Worm	Stable	October 2004
8	Netsky-Q	Win32 Worm	Stable	March 2004
9	Bagle-Z	Win32 Worm	Stable	April 2004
10	Netsky-C	Win32 Worm	Stable	July 2004

Table Updated November 29, 2004

Viruses or Trojans Considered to be a High Level of Threat

- Skulls.B: A second version of the "Skulls" Trojan horse for cell phones has been detected. The hybrid Skulls.B Trojan horse displays images of skulls instead of the program icons on handsets running the Symbian operating system, software maker F-Secure said. Skulls also releases the Cabir.B worm. F-Secure said that cell phones from manufacturers such as Nokia, Siemens, Panasonic and Sendo were vulnerable. F-Secure said that Skulls represents only a mild threat to mobile device users at this point, based on its Trojan horse design. But he said the program is indicative of a growing effort among virus writers to target wireless handsets. For more information see: http://news.com.com/Skulls+program+carries+Cabir+worm+into+phones/2100-7349_3-5469691.html

The following table provides, in alphabetical order, a list of new viruses, variations of previously encountered viruses, and Trojans that have been discovered during the period covered by this bulletin. This information has been compiled from the following anti-virus vendors: Sophos, Trend Micro, Symantec, McAfee, Network Associates, Central Command, F-Secure, Kaspersky Labs, MessageLabs, Panda Software, Computer Associates, and The WildList Organization International. Users should keep anti-virus software up to date and should contact their anti-virus vendors to obtain specific information on the Trojans and Trojan variants that anti-virus software detects.

NOTE: At times, viruses and Trojans may contain names or content that may be considered offensive.

Name	Aliases	Type
Backdoor.Berbew.M		Trojan
Backdoor.Ranky.M		Trojan
Jabbit.A	JS.Jabbit.a JS/Jabbit.A	Java Script Worm
JS.Jabbit		Javascript Virus
PE_LOVEGATE.AC		Trojan
QLowZones-2		Trojan
Skulls.B	SymbOS/Skulls.B	Symbian OS virus
Spawn-C		JavaScript Worm
StartPage-FK		Trojan
StartPage-FN		Trojan
Symb/Cabir-B		Win32 Worm
Troj/Bancban-AH	TrojanSpy.Win32.Banker.di PWS-Bancban.gen.b	Trojan
Troj/Banker-AN	TrojanSpy.Win32.Banker.cy PWS-Bancban	Trojan
Troj/Dloader-EP	Trojan-Downloader.Win32.Delf.ep	Trojan
Trojan.Favadd		Trojan
W32.Garroch@mm	I-Worm.generic W32/Generic.a@MM	Win32 Worm
W32.Myfip.K		Win32 Worm

W32/Anzae-C	IWorm.Pawur.b Email-Worm.Win32.Pawur.a W32/Anzae.worm.c W32/Anzae.worm.d W32/Tasin.B.worm W32/Tasin.C.worm W32/Anzae-B W32.Inzae.B@mm	Win32 Worm
W32/Delf-IV		Win32 Worm
W32/Forbot-CW	Backdoor.Win32.Wootbot.gen	Win32 Worm
W32/Mugly.a@MM	Mugly.A	Win32 Worm
W32/Mugly.b@MM		Win32 Worm
W32/Netsky-AE	I-Worm.NetSky.aa WORM_NETSKY.Z W32/Netsky.z@MM	Win32 Worm
W32/Sality-H		Win32 Worm
W32/Tibick-A		Win32 Worm
Win32.Dluca.V	TrojanDownloader.Win32.Dluca.gen Win32/Dluca.V.Trojan	Win32 Worm
Win32.Siboco.B	Adware-OMI Trojan.Win32.Small.i Win32/Siboco.B.Trojan	Win32 Worm
Win32.Wintrim.AG	TrojanSpy.Win32.Mslagent Win32/TrojanDownloader.Wintrim.NAE Win32/Wintirm.AG.DLL.Trojan	Win32 Worm
Win32.Zlob.A	Win32/Agent.BU.Downloader.Trojan W32/Agent.BU@dl StartPage-EH Trojan.StartPage TrojanDownloader.Win32.Agent.bh	Win32 Worm

[back to top]

Last updated December 01, 2004